

Ranks of quotients, remainders and p -adic digits of matrices

Mustafa Elsheikh* Andy Novocin* Mark Giesbrecht*

Abstract

For a prime p and a matrix $A \in \mathbb{Z}^{n \times n}$, write A as $A = p(A \text{ quo } p) + (A \text{ rem } p)$ where the remainder and quotient operations are applied element-wise. Write the p -adic expansion of A as $A = A^{[0]} + pA^{[1]} + p^2A^{[2]} + \dots$ where each $A^{[i]} \in \mathbb{Z}^{n \times n}$ has entries between $[0, p-1]$. Upper bounds are proven for the \mathbb{Z} -ranks of $A \text{ rem } p$, and $A \text{ quo } p$. Also, upper bounds are proven for the $\mathbb{Z}/p\mathbb{Z}$ -rank of $A^{[i]}$ for all $i \geq 0$ when $p = 2$, and a conjecture is presented for odd primes.

Keywords: Matrix rank, Integer matrix, Remainder and quotient, p -Adic expansion.

AMS classification: 15A03, 15B33, 15B36, 11C20.

Outline

This paper presents two related results on integer matrices after applying element-wise division with remainder. First, let A be an $n \times n$ integer matrix with rank r over \mathbb{Z} and rank r_0 over $\mathbb{Z}/p\mathbb{Z}$. If $n > p^{r_0}$ then Theorem 1 in Section 1 shows that $\text{rank}(A \text{ rem } p) \leq (p^{r_0} - 1)(p + 1)/(2(p - 1))$ and $\text{rank}(A \text{ quo } p) \leq r + (p^{r_0} - 1)(p + 1)/(2(p - 1))$.

The second result is concerned with the $\mathbb{Z}/p\mathbb{Z}$ -ranks of p -adic digits of an integer matrix. Let $U, S, V \in \mathbb{Z}^{n \times n}$ such that U, V have entries from $\{0, 1\}$, $\det U \det V \not\equiv 0 \pmod{p}$, $S = \text{diag}(1, \dots, 1, 0, \dots, 0)$, r be the rank of S over

*Cheriton School of Computer Science, University of Waterloo, Waterloo, Ontario, Canada (melsheik@uwaterloo.ca, andy@novocin.com, mwg@uwaterloo.ca). Supported by the Natural Sciences and Engineering Research Council (NSERC) of Canada.

$\mathbb{Z}/2\mathbb{Z}$, and $n \geq 2^r$. If $M = USV \in \mathbb{Z}^{n \times n}$, then Theorem 16 in Section 2 shows that rank of $M^{[i]}$ over $\mathbb{Z}/2\mathbb{Z}$ is $\binom{r}{2^i}$ for all $i \geq 1$. A conjecture is presented in Section 2.3 for the same setup, but for p an odd prime.

A result on integer rank of Latin squares is also obtained. Let A be the integer matrix of rank one formed by the outer product between the vector $(1, 2, \dots, p-1)$ and its transpose. Then $A \bmod p$ is a Latin square on the symbols $\{1, \dots, p-1\}$. It is shown in Corollary 10 in Section 1.3 that the integer rank of this Latin square is $(p+1)/2$.

1 Quotient and Remainder Matrices

For any integer n and any prime p , let $n \bmod p$ and $n \text{ quo } p$ denote the (non-negative) remainder and quotient in the Euclidean division $n = qp + r$ where $0 \leq r < p$. The operators $\bmod p$ and $\text{quo } p$ are naturally extended to vectors and matrices using element-wise application.

Throughout, we utilize the notion of Smith normal form of an integer matrix. For any matrix $A \in \mathbb{Z}^{n \times n}$ of rank r , there exist unimodular matrices $U, V \in \mathbb{Z}^{n \times n}$ and a unique $n \times n$ integer matrix $S = \text{diag}(s_1, s_2, \dots, s_n)$ such that $A = USV$. Furthermore, $s_i \mid s_{i+1}$ for all $1 \leq i \leq n$ and $s_i = 0$ for all $r < i \leq n$. S is called the Smith normal form of A . For a discussion on existence and uniqueness of Smith normal form, we refer to the reader to the textbook by Newman [3]. We use two notions of ranks. The integer rank of $A \in \mathbb{Z}^{n \times n}$ is denoted by $\text{rank}(A)$. The rank of the image of A in the finite field $\mathbb{Z}/p\mathbb{Z}$ is denoted by $\text{rank}_p(A)$. Alternatively, if $r = \text{rank}(A)$ and the Smith form of A is $S = \text{diag}(s_1, \dots, s_r, 0, \dots, 0)$, then $\text{rank}_p(A) = r_0$ is the maximal index i such that $p \mid s_i$.

Finally, we use the notation $A_{*,j}$ for the j th column of $A \in \mathbb{Z}^{n \times n}$ and $a_{i,j}$ for the entry (i, j) of A .

1.1 Rank Theorem

The following theorem is the main result of Section 1.

Theorem 1. *Let A be an $n \times n$ matrix over \mathbb{Z} , $r = \text{rank}(A)$, $r_0 = \text{rank}_p(A)$, and assume $n > p^{r_0}$. Then*

- (i) $\text{rank}(A \bmod p) \leq (p^{r_0} - 1)(p + 1)/(2(p - 1))$.
- (ii) $\text{rank}(A \text{ quo } p) \leq r + (p^{r_0} - 1)(p + 1)/(2(p - 1))$.

Proof. We will prove part (i) in Lemma 2. For part (ii), we have $A = (A \text{ rem } p) + p(A \text{ quo } p)$, or $p(A \text{ quo } p) = A - (A \text{ rem } p)$. For matrices $X = Y + Z$, rank is sub-additive and $\text{rank}(X) \leq \text{rank}(Y) + \text{rank}(Z)$. Scaling a matrix by p or -1 does not change its rank. So $\text{rank}(A \text{ quo } p) \leq \text{rank}(A) + \text{rank}(A \text{ rem } p) = r + \text{rank}(A \text{ rem } p)$. \square

Lemma 2. $\text{rank}(A \text{ rem } p) \leq (p^{r_0} - 1)(p + 1)/(2(p - 1))$.

Proof. Let $A = USV$ be the Smith normal form of A , with $S = S_r + pS_q$ where $S_q = S \text{ quo } p$ and $S_r = S \text{ rem } p$. Then

$$A \text{ rem } p = USV \text{ rem } p = (US_rV + pUS_qV) \text{ rem } p = US_rV \text{ rem } p. \quad (1)$$

If $r_0 = \text{rank}_p(A)$ then $S_r = \text{diag}(\sigma_1, \dots, \sigma_{r_0}, 0, \dots, 0)$ where $\sigma_i \in [1, p - 1]$ for all $1 \leq i \leq r_0$. The j th column of $A \text{ rem } p$ is

$$A_{*,j} \text{ rem } p = \left(\sum_{\ell=1}^{r_0} \sigma_\ell v_{\ell,j} U_{*,\ell} \right) \text{ rem } p = \left(\sum_{\ell=1}^{r_0} c_{\ell,j} U_{*,\ell} \right) \text{ rem } p, \quad (2)$$

where $c_{\ell,j} \in [0, p - 1]$. If we only consider the non-zero coefficients $c_{\ell,j}$, then the right-hand side of (2) is an i -term sum $(c_{\ell_1,j} U_{*,\ell_1} + \dots + c_{\ell_i,j} U_{*,\ell_i}) \text{ rem } p$, where $1 \leq i \leq r_0$ and $1 \leq \ell_1 < \ell_2 < \dots < \ell_i \leq r_0$. The coefficients $c_{\ell_k,j}$ are elements in $[1, p - 1]$ which are units modulo p . In particular, we can factor $c_{\ell_1,j}$ from the sum, and re-write (2) as:

$$A_{*,j} \text{ rem } p = (c_{\ell_1,j} (U_{*,\ell_1} + \alpha_{\ell_2,j} U_{\ell_2,j} + \dots + \alpha_{\ell_i,j} U_{*,\ell_i})) \text{ rem } p, \quad (3)$$

where $\alpha_{\ell_k,j} \in [1, p - 1]$ for all k .

Fix some i, j and some non-zero assignment of $\alpha_{\ell_2,j}, \dots, \alpha_{\ell_i,j}$ in (3) and let $\hat{u} = U_{*,\ell_1} + \alpha_{\ell_2,j} U_{\ell_2,j} \dots + \alpha_{\ell_i,j} U_{*,\ell_i}$. Then (3) becomes $A_{*,j} \text{ rem } p = (c_{\ell_1,j} \hat{u}) \text{ rem } p$. There are $p - 1$ possible values for $c_{\ell_1,j}$ and hence the possible values of $A_{*,j} \text{ rem } p$ are:

$$\{\hat{u} \text{ rem } p, (2\hat{u}) \text{ rem } p, ((p - 1)\hat{u}) \text{ rem } p\}. \quad (4)$$

We are interested in getting an upper bound on the rank of this set of vectors. First note that $(xy) \text{ rem } p = (x \text{ rem } p)(y \text{ rem } p) \text{ rem } p$. So $(i\hat{u}) \text{ rem } p = (i(\hat{u} \text{ rem } p)) \text{ rem } p$ for $i \in [1, p - 1]$. Hence the maximal rank one can achieve from (4) occurs when (up to permutation) $\hat{u} \text{ rem } p = (0, 1, 2, \dots, p - 1, \dots)$. The rest of the entries are duplicates from the same range $[0, p - 1]$ by the

pigeonhole principle. Now apply Lemma 3 to conclude that the vectors in (4) have rank at most $(p+1)/2$.

Thus for each i, j and non-zero assignment of $\alpha_{\ell_2, j}, \dots, \alpha_{\ell_i, j}$, there are at most $(p+1)/2$ linearly independent columns of $A \bmod p$. We now count the maximal possible number of distinct $A_{*, j}$'s. There are $\binom{r_0}{i}$ possible ways to select i different columns from the first r_0 columns of U . For each choice, there are $i-1$ coefficients: $\alpha_{\ell_2, j}, \dots, \alpha_{\ell_i, j}$, and $(p-1)^{i-1}$ possible ways to assign their non-zero values from $[1, p-1]$. Each choice gives a set of vectors as in (4) whose rank is at most $(p+1)/2$. Summing over all $i \in [1, r_0]$, the maximal possible rank from the span of columns in (2) is

$$\sum_{i=1}^{r_0} \binom{r_0}{i} (p-i)^{i-1} \frac{p+1}{2} = \frac{p^{r_0} - 1}{p-1} \frac{p+1}{2}, \quad (5)$$

using the binomial theorem. \square

1.2 Remainder of Rank-1 Matrices

In this section we prove the following auxiliary result.

Lemma 3. *Let p be any odd prime, $n \geq p$. Let $u \in \mathbb{Z}^n$ be any non-zero vector where the entries of $u \bmod p$ include $\{1, 2, \dots, p-1\}$. Then the set of vectors $\{u \bmod p, (2u) \bmod p, \dots, ((p-1)u) \bmod p\}$ is linearly dependent and has rank $(p+1)/2$.*

First we prove this result for $n = p-1$. A generalization follows. Let $u = (1, 2, \dots, p-1) \in \mathbb{Z}^{(p-1)}$ and $M \in \mathbb{Z}^{(p-1) \times (p-1)}$ be the rank-1 matrix $M = uu^T$ and $R = M \bmod p$.

Lemma 4. $\text{rank}(R) = (p+1)/2$.

Proof. Lemma 5 shows that $(p+1)/2$ is an upper bound on the rank and Lemma 7 shows that $(p+1)/2$ is a lower bound. \square

Lemma 5. $\text{rank}(R) \leq (p+1)/2$.

Proof. Let $1 \leq j \leq (p-1)/2$ and $1 \leq i \leq p-1$. Write $ij = qp + r$ where $0 \leq r < p$. Also $i, j < p \implies p \nmid i \wedge p \nmid j$, which implies $r \neq 0$. Then $i(p-j) = (i-q-1) + (p-r)$ where $0 < (p-r) < p$. So $ij \bmod p + i(p-j) \bmod p = r + (p-r) = p$. But $R_{i,j} = ij \bmod p$, so for all $1 \leq i \leq (p-1)/2$ we have $R_{*,i} = (p, p, \dots, p)^T - R_{*,p-i}$. Thus there are $(p-1)/2$ linearly dependent columns, and no more than $(p+1)/2$ linearly independent columns. \square

To prove that $(p+1)/2$ is also a lower bound on the rank, it suffices (using Lemma 5) to consider the matrix B of size $(p-1) \times \frac{p+1}{2}$ which is formed by the first $(p-1)/2$ columns of R and the column $\bar{B}_{*,(p+1)/2} = R_{*,(p+1)/2} + R_{*,(p-1)/2} = (p, \dots, p)^T$. The matrix B has the following structure:

$$B = \begin{bmatrix} 1 & 2 & \cdots & \frac{p-1}{2} & p \\ 2 & 4 & \cdots & p-1 & p \\ 3 & 6 \bmod p & \cdots & 3\frac{p-1}{2} \bmod p & p \\ \vdots & \vdots & \ddots & \vdots & \\ (p-1) \bmod p & 2(p-1) \bmod p & \cdots & \frac{(p-1)^2}{2} \bmod p & p \end{bmatrix}.$$

Lemma 6. *Either the right kernel of B is empty, or the first $(p-1)/2$ columns of B are linearly dependent.*

Proof. If the right kernel of B is not empty, then there exists $(p+1)/2$ integers $c_1, \dots, c_{(p+1)/2}$ not identically zero, such that

$$c_1 B_{*,1} + c_2 B_{*,2} + \dots + c_{(p+1)/2} B_{*,(p+1)/2} = 0. \quad (6)$$

Apply this linear combination simultaneously to the first two rows of B to get

$$c_1 + 2c_2 + \dots + c_{(p-1)/2} (p-1)/2 = -c_{(p+1)/2} p \quad (7)$$

$$2c_1 + 4c_2 + \dots + c_{(p-1)/2} (p-1) = -c_{(p+1)/2} p \quad (8)$$

But (7) implies either a contradiction in (8): the right kernel of B is empty, or $c_{(p+1)/2} = 0$ and the first $(p-1)/2$ columns of B are linearly dependent. \square

Lemma 7. $(p+1)/2 \leq \text{rank}(R)$.

Proof. Using Lemma 6, proving a lower bound on the rank of R can be reduced to showing that the first $(p-1)/2$ columns of B are linearly independent. We use induction. Consider the sequence of matrices $B^{(k)}$ formed by the first k columns of B , where $2 \leq k \leq (p-1)/2$. The base case of induction, $B^{(2)}$, has rank 2 which is straightforward to verify. For the inductive case, we assume $B^{(k-1)}$ has rank $k-1$, and use Lemma 9 to deduce that $B^{(k)}$ has rank k . \square

The following lemma is needed before proving Lemma 9.

Lemma 8. *For all $j \geq 1$, $(3j \bmod p) - 3j = -pq$ for some integer $q \geq 0$.*

Proof. Write $3j$ as $3j = qp + r$ where $r = 3j \bmod p$ and $q = 3j \text{ quo } p$. Then $r - 3j = -qp$. \square

Lemma 9. *Let $B^{(k)}$ be the $(p-1) \times k$ integer matrix in proof of Lemma 7. Either $B^{(k)}$ has column rank k , or $B^{(k-1)}$ is rank deficient.*

Proof. If the right kernel of $B^{(k)}$ was not empty, then there exists integers c_1, \dots, c_k not identically zero, such that

$$\begin{bmatrix} 1 & 2 & \cdots & k \\ 2 & 4 & \cdots & 2k \\ 3 & 6 \bmod p & \cdots & (3k) \bmod p \\ & & \ddots & \end{bmatrix} \begin{bmatrix} c_1 \\ \vdots \\ c_k \end{bmatrix} = \begin{bmatrix} 0 \\ \vdots \\ 0 \end{bmatrix}. \quad (9)$$

We then perform the following row operations on the left-hand side of (9): replace (row 3) by (row 3) $- 3 \times$ (row 1), then divide row 3 by $-p$. From Lemma 8, we have that row 3 is now

$$[0 \quad \cdots \quad 0 \quad 1 \quad \cdots \quad 1 \quad 2 \cdots \quad q],$$

for some q (in fact, $q = (3k) \text{ quo } p$). We then perform the following column operations: let ℓ denote the column index where the first 1 appears in row 3 (ℓ is guaranteed to be greater than or equal 1 since for all $p > 3$, $k \leq (p-1)/2$, we have $3k > p$.) Pivot on entry ℓ in row 3 and eliminate all entries of row 3 with indices between $\ell + 1$ and $k - 1$. Subtract $q - 1$ multiples of column ℓ from column k . Then pivot on entry k of row 3 and subtract column k from column ℓ . Effectively, this sequence of operations transforms row 3 into:

$$[0 \quad \cdots \quad 0 \quad 1].$$

The right-hand side of (9) is zero, and hence not effected by the aforementioned elementary operations.

Finally, the transformed row 3 implies either that c_k is zero, or the existence of c_1, \dots, c_k is contradictory. This proves the statement of the lemma. \square

We are now ready to generalize Lemma 4 and prove Lemma 3.

Proof of Lemma 3. For the column vector $u \in \mathbb{Z}^{n \times 1}$, consider the matrix $\widehat{R} \in \mathbb{Z}^{n \times n} = uu^T \bmod p$, which is analogous to the matrix R of Lemma 4.

The image of $u \bmod p$ has entries from the interval $[0, p-1]$. If $n > p$ then, by the pigeonhole principle, the vector $u \bmod p$ will contain duplicate (and zero) entries, which correspond to duplicate and zero rows in \widehat{R} . So up to row/column permutations, \widehat{R} contains R as a submatrix, and the extra rows/columns are duplicate and/or zero. Hence $\text{rank}(\widehat{R}) = \text{rank}(R)$. \square

1.3 A Note on Ranks of Latin Squares

It is worth noting that Lemma 4 also implies a result on the ranks of Latin squares of certain orders. As before, let p be an odd prime, and let R be the $(p-1) \times (p-1)$ integer matrix whose (i, j) th entry is $ij \bmod p$. We show that R is a Latin square as follows. R is the Cayley multiplication table of the finite field $\mathbb{Z}/p\mathbb{Z}$, excluding the element 0. Since $\mathbb{Z}/p\mathbb{Z}$ is an integral domain, we have $ij \bmod p \neq i'j' \bmod p$ whenever $j \neq j'$ (where $i, j, j' \in [1, p-1]$). So every row/column of R has the residues $\{1, \dots, p-1\}$ appearing only once, and R is a Latin square of order $p-1$. R has rank 1 over $\mathbb{Z}/p\mathbb{Z}$ and non-trivial rank over \mathbb{Z} by Lemma 4 as stated in the following corollary.

Corollary 10. *Let p be any odd prime, and let R be any Latin square of order $p-1$ on the symbols $\{1, \dots, p-1\}$. Then the integer rank of R , taken as a $(p-1) \times (p-1)$ integer matrix, is $(p+1)/2$.*

2 p -adic Matrices

We now switch the focus to ranks of p -adic matrices. Ranks in this section are over the finite field with p elements*, with residue classes $\{0, 1, \dots, p-1\}$. For any prime p and any matrix $M \in \mathbb{Z}^{n \times n}$ with entries $|m_{i,j}| < \beta$, the p -adic expansion of M is $M = M^{[0]} + pM^{[1]} + \dots + p^s M^{[s]}$ where the entries of each matrix $M^{[i]}$ are between $[0, p-1]$, and $s \leq \lceil \log_p \beta \rceil$. We call $M^{[i]}$ the i th p -adic matrix digit of M . We extend the superscript $[i]$ notation to vectors and integers in the obvious way.

We present results concerning the 2-adic matrix digits. For odd primes, we only present a conjecture. It is an open question to study the combinatorial structure of the column space of the p -adic matrix digits for primes other than 2.

*The two ranks, over \mathbb{Z} and over $\mathbb{Z}/p\mathbb{Z}$, are equal unless p is an elementary divisor of the matrix.

$$\begin{bmatrix}
0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 \\
0 & 0 & 1 & 0 \\
0 & 1 & 0 & 0 \\
1 & 0 & 0 & 0 \\
\hline
0 & 0 & 1 & 1 \\
0 & 1 & 0 & 1 \\
0 & 1 & 1 & 0 \\
1 & 0 & 0 & 1 \\
1 & 0 & 1 & 0 \\
1 & 1 & 0 & 0 \\
\hline
0 & 1 & 1 & 1 \\
1 & 0 & 1 & 1 \\
1 & 1 & 0 & 1 \\
1 & 1 & 1 & 0 \\
\hline
1 & 1 & 1 & 1
\end{bmatrix},
\begin{bmatrix}
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 1 \\
0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 \\
0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 1 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 \\
\hline
0 & 1 & 1 & 0 & 0 & 2 & 1 & 1 & 1 & 1 & 0 & 2 & 2 & 1 & 1 & 2 \\
0 & 1 & 0 & 1 & 0 & 1 & 2 & 1 & 1 & 0 & 1 & 2 & 1 & 2 & 1 & 2 \\
0 & 0 & 1 & 1 & 0 & 1 & 1 & 2 & 0 & 1 & 1 & 2 & 1 & 1 & 2 & 2 \\
0 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 2 & 1 & 1 & 1 & 2 & 2 & 1 & 2 \\
0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 2 & 1 & 1 & 2 & 1 & 2 & 2 \\
0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 2 & 1 & 1 & 2 & 2 & 2 \\
\hline
0 & 1 & 1 & 1 & 0 & 2 & 2 & 2 & 1 & 1 & 1 & 3 & 2 & 2 & 2 & 3 \\
0 & 1 & 1 & 0 & 1 & 2 & 1 & 1 & 2 & 2 & 1 & 2 & 3 & 2 & 2 & 3 \\
0 & 1 & 0 & 1 & 1 & 1 & 2 & 1 & 2 & 1 & 2 & 2 & 2 & 3 & 2 & 3 \\
0 & 0 & 1 & 1 & 1 & 1 & 1 & 2 & 1 & 2 & 2 & 2 & 2 & 2 & 3 & 3 \\
\hline
0 & 1 & 1 & 1 & 1 & 2 & 2 & 2 & 2 & 2 & 2 & 3 & 3 & 3 & 3 & 4
\end{bmatrix}$$

Figure 1: An example of A (left) and $M = AA^T$ (right), where $r = 4$. The rows of A are partitioned by the number of non-zero entries in each row. The corresponding blocks in the symmetric matrix M are shown with borders. The column partitions of M are $\mathbf{m}_0, \mathbf{m}_1, \mathbf{m}_2, \mathbf{m}_3, \mathbf{m}_4$. And $\text{rank}_p(M^{[0]}) = \text{rank}_p(\mathbf{m}_1^{[0]}) = 4$, $\text{rank}_p(M^{[1]}) = \text{rank}_p(\mathbf{m}_2^{[1]}) = 6$, $\text{rank}_p(M^{[2]}) = \text{rank}_p(\mathbf{m}_4^{[2]}) = 1$.

2.1 Binary code matrices

Fix $p = 2$. The goal of this section is to show that for all $i \geq 1$, $\text{rank}_p(M^{[i]}) = \binom{r}{2^i}$ where $M = AA^T$ for some specially constructed A , which we call *binary code matrix*. We will generalize the construction of M in a subsequent section. For now, A is constructed as follows. Start with the $2^r \times r$ matrix whose i, j entry is the j th bit in the binary expansion of i . Then apply row permutations to A such that the first $\binom{r}{0}$ rows have exactly 0 non-zero entries, followed by $\binom{r}{1}$ rows which have exactly 1 non-zero entries, followed by $\binom{r}{2}$ rows which have exactly 2 non-zero entries and so on. See Figure 2.1 for an example where $r = 4$.

The ℓ th column of M is given by:

$$M_{*,\ell} = a_{1,\ell}A_{*,1} + \dots + a_{r,\ell}A_{*,r} = \sum_{j \in J_\ell} A_{*,j}, \quad (10)$$

where $J_\ell \subseteq \{1, 2, \dots, r\}$ and the second equality holds because $a_{i,\ell} \in \{0, 1\}$. We call J_ℓ the *summing index set* of $M_{*,\ell}$. Let \mathbf{m}_k denote the $2^r \times \binom{r}{k}$ submatrix of M , which includes all columns of the form: $M_{*,\ell} = \sum_{j \in J_\ell} A_{*,j}$ where $J_\ell \subseteq \{1, 2, \dots, r\}$ and $|J_\ell| = k$. Then the columns of M can be partitioned into:

$$M = [\mathbf{m}_0 \quad \mathbf{m}_1 \quad \mathbf{m}_2 \quad \dots \quad \mathbf{m}_{2^i} \quad \mathbf{m}_{2^i+1} \quad \dots \quad \mathbf{m}_r]. \quad (11)$$

The next lemma shows that

$$M^{[i]} = \begin{bmatrix} \mathbf{0} & \mathbf{0} & \dots & \mathbf{0} & \mathbf{m}_{2^i}^{[i]} & \mathbf{m}_{2^i+1}^{[i]} & \dots & \mathbf{m}_r^{[i]} \end{bmatrix}. \quad (12)$$

Lemma 11. *If $k < 2^i$, then $\mathbf{m}_k^{[i]} = \mathbf{0}$ for all $i \geq 1$.*

Proof. Columns of \mathbf{m}_k are given by $\sum_{j \in J} A_{*,j}$ where $|J| = k$. The entries of A are either 0 or 1. So the largest entry in \mathbf{m}_k is $1 + \dots + 1 = k$. The result follows by appealing to the binary expansion of k . \square

We expect $\text{rank}_p(\mathbf{m}_{2^i}^{[i]}) \leq \binom{r}{2^i}$ since $\mathbf{m}_{2^i}^{[i]}$ is a matrix of dimension $2^r \times \binom{r}{2^i}$. The next lemma shows that the rank is, in fact, equal to this upper bound.

Lemma 12. $\text{rank}_p(\mathbf{m}_{2^i}^{[i]}) = \binom{r}{2^i}$ for all $i \geq 1$.

Proof. Let $c_1, \dots, c_{\binom{r}{2^i}}$ be the column indices of \mathbf{m}_{2^i} in M . Let $S(\mathbf{m}_{2^i})$ be the $\binom{r}{2^i} \times \binom{r}{2^i}$ submatrix of \mathbf{m}_{2^i} formed by the rows $c_1, \dots, c_{\binom{r}{2^i}}$, and $S(A)$ be the $\binom{r}{2^i} \times r$ submatrix of A formed by the rows $c_1, \dots, c_{\binom{r}{2^i}}$. Rows of $S(A)$ have exactly 2^i non-zero entries because of the construction of A . If we treat A and M as block matrices then $S(\mathbf{m}_{2^i}) = S(A)S(A)^T$ is the 2^i th diagonal block of M (See Figure 2.1).

The entries in row ρ of $S(\mathbf{m}_{2^i})$ are given by linear combinations of the entries in row ρ of $S(A)$. The summing index sets J_j , where $|J_j| = 2^i$, are exactly the locations of the non-zero entries of rows of $S(A)$, which are all *different* by construction. Hence there is only one entry in row ρ of $S(\mathbf{m}_{2^i})$ whose summing set matches the locations of the non-zero entries in row ρ of

$S(A)$. The value of this entry is $1 + 1 + \dots + 1 = 2^i$. The other entries have values less than 2^i . Now appeal to the binary expansion of 2^i to get that $S(\mathbf{m}_{2^i}^{[i]})$ is an identity (sub)matrix[†] of $\mathbf{m}_{2^i}^{[i]}$ whose size is $\binom{r}{2^i} \times \binom{r}{2^i}$. Therefore, $\mathbf{m}_{2^i}^{[i]}$ has rank $\binom{r}{2^i}$. \square

Next we will prove that $\text{rank}_p(M^{[i]}) = \binom{r}{2^i}$ by showing that all the columns of $\mathbf{m}_{2^{i+1}}^{[i]}, \mathbf{m}_{2^{i+2}}^{[i]}, \dots, \mathbf{m}_{2^r}^{[i]}$ are linearly dependent on those of $\mathbf{m}_{2^i}^{[i]}$.

Lemma 13. *Consider any column m in $\mathbf{m}_{2^i+z}^{[i]}$, where $z \geq 1$. Then $m^{[i]}$ is a linear combination of columns of $\mathbf{m}_{2^i}^{[i]}$.*

Proof. Let J be the summing index set of m , where $|J| = 2^i + z$. Let \mathcal{I} be the set of all subsets of J of size 2^i , so $|\mathcal{I}| = \binom{2^i+z}{2^i}$. For every $I \in \mathcal{I}$, there is a unique corresponding column c_I in $\mathbf{m}_{2^i}^{[i]}$ whose summing set is I . We will show that $m^{[i]}$ can be obtained by adding up c_I 's. In other words,

$$m^{[i]} \equiv \sum_{I \in \mathcal{I}} c_I^{[i]} \pmod{2}. \quad (13)$$

Let A_J denote the submatrix of A formed by the columns indexed by J . For any row ρ of A_J , let $2^i + k_\rho$ be the number of 1's in that row, where $-2^i \leq k_\rho \leq z$. First, if $k_\rho < 0$, then the corresponding sum of 1's at this row is less than 2^i . By Lemma 11, we have the corresponding entries in both $\mathbf{m}_{2^i}^{[i]}$ and $\mathbf{m}_{2^i+z}^{[i]}$ are zeros and (13) trivially holds. On the other hand, if $0 \leq k_\rho \leq z$, then the ρ th entry of the right-hand side of (13) is $1 + 1 + \dots + 1 \equiv \binom{2^i+k_\rho}{2^i} \pmod{2}$ since $|\mathcal{I}| = \binom{2^i+k_\rho}{2^i}$. (Recall that the number of non-zero entries in row ρ is $2^i + k_\rho$ rather than $2^i + z$.) The ρ th entry of the left-hand side of (13) is $(2^i + k_\rho) \text{ quo } 2^i$. The $(2^i + k_\rho)$ term corresponds to adding $(2^i + k_\rho)$ non-zero entries, and the $\text{quo } 2^i$ operation corresponds to the i th bit of the binary expansion of m . By Lemma 15 (below), we have $(2^i + k_\rho) \text{ quo } 2^i \equiv \binom{2^i+k_\rho}{2^i} \pmod{2}$, and (13) holds. \square

The proof of the next (auxiliary) lemma uses a theorem due to Kummer [2].

[†]This is true in the example of Figure 2.1 without any reordering, because we constructed the row blocks of A such that the binary expansion of i comes after the binary expansion of j whenever $i > j$. Without such ordering, the identity block assertion holds up to row and column permutations.

Fact 14 (Kummer's Theorem). *The exact power of p dividing $\binom{a+b}{a}$ is equal to the number of carries when performing the addition of $(a+b)$ written in base p .*

A corollary of Kummer's theorem is that $\binom{a+b}{a}$ is odd (resp. even) if adding $(a+b)$ written in binary expansion generates no (resp. some) carries.

Lemma 15. $(2^i + k) \text{ quo } 2^i \equiv \binom{2^i+k}{2^i} \pmod{2}$.

Proof. We will show that $(2^i + k) \text{ quo } 2^i$ and $\binom{2^i+k}{2^i}$ have the same parity. Write $k = Q2^i + R$ for a quotient $Q \geq 0$ and a remainder $0 \leq R < 2^i$. There are two cases for Q . If Q is even, then the i th bit[‡] of k is 0 and hence no carries are generated when adding k and 2^i in base 2. So by Kummer's Theorem, $\binom{2^i+k}{2^i}$ is odd and $\binom{2^i+k}{2^i} \equiv 1 \pmod{2}$. If Q is odd, then the i th bit of k is 1 and the number of carries generated when adding $2^i + k$ in base 2 is at least 1. So by Kummer's theorem $\binom{2^i+k}{2^i}$ is even and $\binom{2^i+k}{2^i} \equiv 0 \pmod{2}$.

We have shown that $\binom{2^i+k}{2^i}$ and Q have opposite parities. Now, substitute $k = Q2^i + R$ to get $(2^i + k) \text{ quo } 2^i = Q + 1$. Hence, modulo 2, $(2^i + k) \text{ quo } 2^i$ also have an opposite parity to that of Q . This concludes our proof. \square

2.2 Non-symmetric Matrices

So far we have shown that $\text{rank}_p(M^{[i]}) = \text{rank}_p(\mathbf{m}_{2^i}^{[i]}) = \binom{r}{2^i}$, where $M = AA^T$ for some specially constructed A . We now put the results together into a more general theorem.

Theorem 16. *Assume $U, S, V \in \mathbb{Z}^{n \times n}$, such that U, V have entries from $\{0, 1\}$, $\det U \det V \not\equiv 0 \pmod{2}$, $S = \text{diag}(1, \dots, 1, 0, \dots, 0)$, $\text{rank}_p(S) = r$, and $n \geq 2^r$. If $M = USV \in \mathbb{Z}^{n \times n}$, then $\text{rank}_p(M^{[i]}) = \binom{r}{2^i}$ for all $i \geq 1$.*

Proof. Since $S = SS$, we have $M = USV = USSV = LR$, where $L = US \in \mathbb{Z}^{n \times r}$, and $R = SV \in \mathbb{Z}^{r \times n}$. Let $A \in \mathbb{Z}^{2^r \times r}$ be the binary code matrix of the digits $\{0, \dots, 2^r - 1\}$. Consider the matrices $\hat{L} = A$, $\hat{R} = A^T$ and $\hat{M} = \hat{L}\hat{R}$. If we start with \hat{L} (resp. \hat{R}) and augment it with the appropriate $(n - 2^r)$ additional rows (resp. columns), and apply the appropriate row and column permutations, then we could transform \hat{L} into L (resp. \hat{R} into R), and in effect, transform \hat{M} into M . Our goal is to show that the rank arguments of the previous lemmas hold under the aforementioned operations.

[‡]i.e. the coefficient of 2^i in the binary expansion of k .

We first note that row and column permutations preserve ranks. Also, by a simple enumeration argument over the binary tuples of size r , and by the given fact that $n \geq 2^r$, we can conclude that any additional rows (resp. columns) augmented to \widehat{L} (resp. \widehat{R}) will be linearly dependent. In fact, any such rows (resp. columns) will be duplicates of existing rows (resp. columns).

Now, consider adding extra columns to \widehat{R} . The resulting extra columns in \widehat{M} are duplicates of existing columns and hence the ranks in Lemma 12 are not affected. Finally, adding extra rows to \widehat{L} does not change the cardinality of the summing index sets in (10). The rest of the results are straightforward to verify. \square

2.3 Odd Primes

For $p = 2$, the non-zero patterns of the binary code matrix A coincides with the summing indices in (10). This is not true for odd primes, where the linear combinations can have coefficients other than 0 and 1. Thus it is an open question to devise construction a similar to binary code matrices, which exposes the combinatorial structure of the column space of $M = AA^T$. However, we present the following conjecture towards understanding the p -adic ranks for odd primes.

Conjecture 17. *Assume $p = 2k + 1$ is an odd prime, $U, S, V \in \mathbb{Z}^{n \times n}$ such that U, V have entries from $[0, p - 1]$, $\det U \det V \not\equiv 0 \pmod{p}$, S is a $0, 1$ diagonal matrix and $\text{rank}_p(S) = r$. Let $M = USV = M^{[0]} + M^{[1]}p + \dots$ where $M^{[i]} \in (\mathbb{Z}/p\mathbb{Z})^{n \times n}$. It is conjectured that*

$$\text{rank}_p(M^{[1]}) \leq \sum_{i=0}^k \binom{r + 2i}{2i + 1} + \binom{r + 2k - 1}{2k} - 2r \quad (14)$$

Furthermore, in the generic case where the entries of U, V are uniformly chosen at random from $[0, p - 1]$, and n is arbitrarily large, the ranks are equal to the stated bound.

This conjecture first appeared in [1]. It shows that a product of matrices with “small” entries and “small” rank can still have very large rank, but not full, p -adic expansion. In other words, the “carries” from the product USV will impact many digits in the expanded product.

Acknowledgment

The authors would like to thank Andrew Arnold, Kevin Hare, David McKinnon, Jason Peasgood, and B. David Saunders.

References

- [1] M. Elsheikh, M. Giesbrecht, A. Novocin, and B. D. Saunders. Fast computation of Smith forms of sparse matrices over local rings. In *Proceedings of the 37th International Symposium on Symbolic and Algebraic Computation*, ISSAC '12, pages 146–153, New York, NY, USA, 2012. ACM.
- [2] E. E. Kummer. Über die Ergänzungssätze zu den allgemeinen Reciprocitätsgesetzen. *Journal für die reine und angewandte Mathematik*, 44:93–146, 1851.
- [3] M. Newman. *Integral Matrices*. Academic Press, New York, NY, USA, 1972.